

JP7036672

Publication Title:

**RANDOM-NUMBER GENERATOR, COMMUNICATION SYSTEM USING THE
SAME AND METHOD THEREFOR**

Abstract:

PURPOSE:To generate a safe random number sequence at a high speed.

CONSTITUTION:This generator is provided with a shift register 1 bonding data, a linear conversion circuit 12 inputting the data held in the shift register 11 and converting an inputted data value based on a prescribed parameter, an update means updating the data held in the shift register 11 based on the conversion result by the linear conversion circuit 12 and an output means successively outputting the partial data held in the shift register 11 as a random number sequence.

Data supplied from the esp@cenet database - <http://ep.espacenet.com>

This Patent PDF Generated by Patent Fetcher(TM), a service of Patent Logistics, LLC

Patent provided by Sughrue Mion, PLLC - <http://www.sughrue.com>

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開平7-36672

(43) 公開日 平成7年(1995)2月7日

(51) Int.Cl. ⁶	識別記号	庁内整理番号	F I	技術表示箇所
G 0 6 F 7/58	C			
G 0 9 C 1/00		8837-5L		
H 0 4 L 9/22				
			H 0 4 L 9/ 04	

審査請求 未請求 請求項の数 6 O L (全 12 頁)

(21) 出願番号 特願平5-179232

(22) 出願日 平成5年(1993)7月20日

(71) 出願人 000001007

キヤノン株式会社

東京都大田区下丸子3丁目30番2号

(72) 発明者 山本 貴久

東京都大田区下丸子3丁目30番2号キヤノン株式会社内

(72) 発明者 岩村 恵市

東京都大田区下丸子3丁目30番2号キヤノン株式会社内

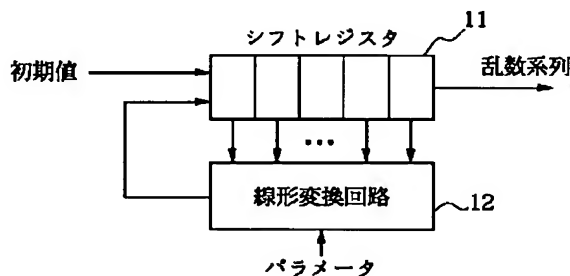
(74) 代理人 弁理士 丸島 儀一

(54) 【発明の名称】 乱数発生器、及びそれを用いた通信システム及びその方法

(57) 【要約】

【目的】 高速かつ安全な乱数系列を発生する。

【構成】 データを保持するシフトレジスタ11と、該シフトレジスタ11に保持されたデータを入力し、所定のパラメータに基づいて入力データ値を変換する線形変換回路12と、該線形変換回路12による変換結果に基づき、前記シフトレジスタ11に保持されるデータを更新する更新手段と、前記シフトレジスタ11に保持されるデータの一部を、乱数系列として順次出力する出力手段とを具える。



1

【特許請求の範囲】

【請求項1】 データを保持する保持手段と、

該保持手段に保持されたデータを入力し、所定のパラメータに基づいて入力データ値を変換する変換手段と、
 該変換手段による変換結果に基づき、前記保持手段に保持されるデータを更新する更新手段と、
 前記保持手段に保持されるデータの一部を、乱数系列として順次出力する出力手段とを具え、前記パラメータを所定の周期で変更することを特徴とする乱数発生器。

【請求項2】 データを保持する保持手段と、

該保持手段に保持されたデータを入力し、所定のパラメータに基づいて入力データ値を変換する変換手段と、
 該変換手段による変換結果に基づき、前記保持手段に保持されるデータを更新する更新手段と、
 前記保持手段に保持されるデータの一部を、乱数系列として順次出力する出力手段と、
 前記パラメータとして出力系列から該系列を推定することが困難なパラメータ系列を順次算出してパラメータを変更する算出手段とを具えることを特徴とする乱数発生器。

【請求項3】 データを保持する第1の保持手段と、

該第1の保持手段に保持されたデータを入力し、所定のパラメータに基づいて入力データ値を変換する第1の変換手段と、
 該第1の変換手段による変換結果に基づき、前記第1の保持手段に保持されるデータを更新する第1の更新手段と、
 前記第1の保持手段に保持されるデータの一部を、乱数系列として順次出力する第1の出力手段と、
 該第1の出力手段より出力される乱数系列に基づいて通信文を暗号化する暗号化手段とを送信装置に具え、
 データを保持する第2の保持手段と、
 該第2の保持手段に保持されたデータを入力し、所定のパラメータに基づいて入力データ値を変換する第2の変換手段と、
 該第2の変換手段による変換結果に基づき、前記第2の保持手段に保持されるデータを更新する第2の更新手段と、
 前記第2の保持手段に保持されるデータの一部を、乱数系列として順次出力する第2の出力手段と、
 該第2の出力手段より出力される乱数系列に基づいて暗号文を復号する復号手段とを受信装置に具えたことを特徴とする通信システム。

【請求項4】 データを保持する第1の保持手段と、

該第1の保持手段に保持されたデータを入力し、所定のパラメータに基づいて入力データ値を変換する第1の変換手段と、
 該第1の変換手段による変換結果に基づき、前記第1の保持手段に保持されるデータを更新する第1の更新手段と、

2

前記第1の保持手段に保持されるデータの一部を、乱数系列として順次出力する第1の出力手段と、

前記パラメータとして出力系列から該系列を推定することが困難なパラメータ系列を順次算出してパラメータを変更する第1の算出手段と、

前記第1の出力手段より出力される乱数系列に基づいて通信文を暗号化する暗号化手段とを送信装置に備え、

データを保持する第2の保持手段と、

10 該第2の保持手段に保持されたデータを入力し、所定のパラメータに基づいて入力データ値を変換する第2の変換手段と、

該第2の変換手段による変換結果に基づき、前記第2の保持手段に保持されるデータを更新する第2の更新手段と、

前記第2の保持手段に保持されるデータの一部を、乱数系列として順次出力する第2の出力手段と、

前記パラメータとして出力系列から該系列を推定することが困難なパラメータ系列を順次算出してパラメータを変更する第2の算出手段と、

20 前記第2の出力手段より出力される乱数系列に基づいて暗号文を復号する復号手段とを受信装置に具えたことを特徴とする通信システム。

【請求項5】 送信側で、データを保持する第1の保持部に保持されたデータを第1の変換部に入力し、

所定のパラメータに基づいて入力データを変換し、

該変換の結果に基づき、前記第1の保持部に保持されるデータを更新し、

前記第1の保持部に保持されるデータの一部を、乱数系列として順次出力し、

30 該出力される乱数系列に基づいて通信文を暗号化して暗号文を順次受信側に送信し、

受信側で、データを保持する第2の保持部に保持されたデータを第2の変換部に入力し、

所定のパラメータに基づいて入力データを変換し、

該変換の結果に基づき、前記第2の保持部に保持されるデータを更新し、

前記第2の保持部に保持されるデータの一部を、乱数系列として順次出力し、

40 該出力される乱数系列に基づいて暗号文を復号することを特徴とする通信方法。

【請求項6】 送信側で、データを保持する第1の保持部に保持されたデータを第1の変換部に入力し、

所定のパラメータに基づいて入力データを変換し、

該変換の結果に基づき、前記第1の保持部に保持されるデータを更新し、

前記パラメータとして出力系列から該系列を推定することが困難なパラメータ系列を順次算出してパラメータを変更し、

50 前記第1の保持部に保持されるデータの一部を、乱数系列として順次出力し、

3

該出力される乱数系列に基づいて通信文を暗号化する暗号文を順時受信側に送信し、

受信側で、データを保持する第2の保持部に保持されたデータを第2の変換部に入力し、

所定のパラメータに基づいて入力データを変換し、

該変換の結果に基づき、前記第2の保持部に保持されるデータを更新し、

前記パラメータとして出力系列から該系列を推定することが困難なパラメータ系列を順次算出してパラメータを更新し、

前記第2の保持部に保持されるデータの一部を、乱数系列として順次出力し、

該出力される乱数系列に基づいて暗号文を復号することを特徴とする通信方法。

【発明の詳細な説明】

【0001】

【産業上の利用分野】本発明は暗号化方式に関係し、特に暗号通信分野におけるデータの秘匿、発信者・着信者の認証、暗号鍵の共有、零知識証明プロトコル等に関するものである。また、モンテカルロシミュレーションなどの乱数を用いたシミュレーションに関するものである。

【0002】

【従来の技術】従来、乱数発生法の一つとして、文献「現代暗号理論」（池野、小山著、昭和61年発行、電子情報通信学会）の第69～72頁に示されているように、最大長周期系列（M系列）を発生する線形フィードバックシフトレジスタ（LFSR）を用いたものが知られている。

【0003】LFSR方式とは、図14に示すようにs段のシフトレジスタ $R(t) = (r_s(t), r_{s-1}(t), \dots, r_2(t), r_1(t))$ とタップ（引込線）列 $(h_s, h_{s-1}, \dots, h_2, h_1)$ からなり、各時点（ストップ）ごとに次のような動作を同時に行うことにより、擬似乱数系列を生成する方法である。

【0004】(a) 最右端のレジスタのビット $r_1(t)$ を擬似乱数系列として出力する。

【0005】 $k_i = r_1(t)$

(b) $r_s(t), r_{s-1}(t), \dots, r_2(t)$ を右にシフトする。

【0006】 $r_i(t+1) = r_{i+1}(t) \quad (i=1, 2, \dots, s-1)$

(c) 最左端のレジスタのビット $r_s(t+1)$ をレジスタの内容とタップ列により、次のように計算する。

【0007】

【外1】

$$r_s(t+1) = \sum_{i=1}^s h_i \cdot r_i(t) \bmod 2$$

以上まとめると、LFSR方式の擬似乱数発生アルゴリズムはs行s列の行列Hを用いて、

4

$$R(t+1) = H \cdot R(t) \bmod 2 \quad (1)$$

つまり、

【0008】

【外2】

$$\begin{bmatrix} r_s(t+1) \\ r_{s-1}(t+1) \\ r_{s-2}(t+1) \\ \vdots \\ r_2(t+1) \\ r_1(t+1) \end{bmatrix} = \begin{bmatrix} h_s & h_{s-1} & \cdots & h_2 & h_1 \\ 1 & 0 & \cdots & 0 & 0 \\ 0 & 1 & \cdots & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & 1 & 0 \\ 0 & 0 & \cdots & 0 & 1 \end{bmatrix} \begin{bmatrix} r_s(t) \\ r_{s-1}(t) \\ r_{s-2}(t) \\ \vdots \\ r_2(t) \\ r_1(t) \end{bmatrix}$$

と表せる。

【0009】このs段のLFSRのタップ列をうまく選ぶと、最大周期 $2^s - 1$ の擬似乱数のビット系列を生成することができ、その時の系列が前述の最大長周期系列となる。

【0010】しかしながら、このLFSRを用いる乱数発生法では、LFSRの線形性を利用して2sビットの出力擬似乱数系列からs段のタップ列 $(h_s, h_{s-1}, \dots, h_2, h_1)$ を以下の方法で決定できる。

【0011】出力される擬似乱数系列が k_1, k_2, \dots, k_{2s} であったとすると、ある時点t ($t=1, 2, \dots, s+1$)のレジスタの内容 $R(t)$ は、

$$R(1) = (k_s, k_{s-1}, \dots, k_1)^T$$

$$R(2) = (k_{s+1}, k_s, \dots, k_2)^T$$

...

$$R(s+1) = (k_{2s}, k_{2s-1}, \dots, k_{s+1})^T$$

と表せる（ T は転置を示す）。この時、行列X、Yを

$$X = (R(1), R(2), \dots, R(s))$$

$$Y = (R(2), R(3), \dots, R(s+1))$$

とすると、式(1)より

$$Y = H \cdot X$$

の関係が成立するため、

$$H = Y \cdot X^{-1} \quad (2)$$

によりHが求められ、タップ列が決定される。

【0012】つまり、乱数の周期は $2^s - 1$ であるがそのうち2sビットでLFSRの構成が決定される。この場合、その時点以降に発生される乱数系列が全てわかってしまうため、出力乱数系列を暗号用の乱数として用いるには安全性の面で不適当であるという欠点があった。

【0013】また、非線形フィードバックシフトレジスタを用いれば、出力乱数系列の解析に必要な乱数の数を大きくすることができると知られている。しかし、バーレカンブ・マッセイのアルゴリズム（E. R. Berlekamp "Algebraic coding theory", McGraw-Hill Book Company, 1968）によりその系列を生成することができる最小段数のLFSRを求めることがで

き、非線形フィードバックシフトレジスタを用いた乱数発生方式も、式(2)の方法により解析される可能性があった。

【0014】以上の様に、ある時点までの出力乱数を手に入れることができれば、それ以降に出力する乱数列全てを容易に予測することができる乱数発生方式を便宜上方式Aと呼ぶことにする。方式Aは上述のように暗号学的に安全ではないが、構成が容易なので高速処理が可能であるという特徴を持つ。

【0015】方式Aとは異なり、ある時点までに発生さ* 10

$$x_{i+1} = x_i^2 \bmod n \quad (i=0, 1, 2, \dots) \quad (3)$$

$b_i = \text{l s b}(x_i) \quad (i=0, 1, 2, \dots)$

によって与えられる(ただし、 $n=p \cdot q$ 、 l s b は最下位ビットを表す)。

【0017】この方法により生成された乱数列 b_1, b_2, \dots, b_i のみから b_{i+1} を求めることは、 n を因数分解するのと同じだけの手間が必要であることが知られている。つまり、ある時点までに発生された乱数列のみからその時点以降に発生されるべき乱数を求めるための計算量は、 n を因数分解するのに必要な計算量と同等であることが知られている。ただし、 n を因数分解することを計算量的に困難にするためには p, q を数百ビット程度にする必要がある。このように、ある時点までに発生された乱数列のみからその時点以降に発生されるべき乱数を予測することが計算量的に困難となるような方法により生成された乱数は、暗号学的に安全な擬似乱数と呼ばれている。

【0018】しかし、乱数発生法として暗号学的に安全な擬似乱数発生方式を用いた場合には、前述のように p, q を数百ビット程度にする必要があり、その場合、式(3)の $x_{i+1} = x_i^2 \bmod n$ を計算するための計算量が大きく、高速に乱数を発生できないという問題があった。

【0019】

【課題を解決するための手段】上記課題を解決するために、本発明の乱数発生器は、データを保持する保持手段と、該保持手段に保持されたデータを入力し、所定のパラメータに基づいて入力データ値を変換する変換手段と、該変換手段による変換結果に基づき、前記保持手段に保持されるデータを更新する更新手段と、前記保持手段に保持されるデータの一部を、乱数系列として順次出力する出力手段とを具える。

【0020】また、本発明の他の態様によれば、データを保持する保持手段と、該保持手段に保持されたデータを入力し、所定のパラメータに基づいて入力データ値を変換する変換手段と、該変換手段による変換結果に基づき、前記保持手段に保持されるデータを更新する更新手段と、前記保持手段に保持されるデータの一部を、乱数系列として順次出力する出力手段と、前記パラメータとして出力系列から該系列を推定することが困難なパラメ

*れた乱数列のみからその時点以降に発生されるべき乱数を予測することが非常に困難となる乱数発生法を以下に示し、便宜上方式Bと呼ぶことにする。

【0016】方式Bの実現方法として、文献「アドバンセズ・イン・クリプトロジー」(“Advances in Cryptology”, 1983年発行、PLENUM PRESS, 61~78項)に示されているような方法が知られている。つまり、乱数列を b_1, b_2, \dots とするとビット b_i は、 x_0 を任意に与える初期値、 p, q を素数として、

一タ系列を順次算出してパラメータを変更する算出手段とを具える。

【0021】また、本発明の他の態様によれば、データを保持する第1の保持手段と、該第1の保持手段に保持されたデータを入力し、所定のパラメータに基づいて入力データ値を変換する第1の変換手段と、該第1の変換手段による変換結果に基づき、前記第1の保持手段に保持されるデータを更新する第1の更新手段と、前記第1の保持手段に保持されるデータの一部を、乱数系列として順次出力する第1の出力手段と、該第1の出力手段より出力される乱数系列に基づいて通信文を暗号化する暗号化手段とを送信装置に具え、データを保持する第2の保持手段と、該第2の保持手段に保持されたデータを入力し、所定のパラメータに基づいて入力データ値を変換する第2の変換手段と、該第2の変換手段による変換結果に基づき、前記第2の保持手段に保持されるデータを更新する第2の更新手段と、前記第2の保持手段に保持されるデータの一部を、乱数系列として順次出力する第2の出力手段と、該第2の出力手段より出力される乱数系列に基づいて暗号文を復号する復号手段とを受信装置に具える。

【0022】また、本発明の他の態様によれば、データを保持する第1の保持手段と、該第1の保持手段に保持されたデータを入力し、所定のパラメータに基づいて入力データ値を変換する第1の変換手段と、該第1の変換手段による変換結果に基づき、前記第1の保持手段に保持されるデータを更新する第1の更新手段と、前記第1の保持手段に保持されるデータの一部を、乱数系列として順次出力する第1の出力手段と、前記パラメータとして出力系列から該系列を推定することが困難なパラメータ系列を順次算出してパラメータを変更する第1の算出手段と、前記第1の出力手段より出力される乱数系列に基づいて通信文を暗号化する暗号化手段とを送信装置に具え、データを保持する第2の保持手段と、該第2の保持手段に保持されたデータを入力し、所定のパラメータに基づいて入力データ値を変換する第2の変換手段と、該第2の変換手段による変換結果に基づき、前記第2の保持手段に保持されるデータを更新する第2の更新手段と、前記第2の保持手段に保持されるデータの一部を、

乱数系列として順次出力する第2の出力手段と、前記パラメータとして出力系列から該系列を推定することが困難なパラメータ系列を順次算出してパラメータを変更する第2の算出手段と、前記第2の出力手段より出力される乱数系列に基づいて暗号文を復号する復号手段とを受信装置に具える。

【0023】

【作用】かかる本発明の乱数発生器においては、保持手段に保持されたデータを入力し、所定のパラメータに基づいて入力データ値を変換手段により変換し、該変換手段による変換結果に基づき、前記保持手段に保持されるデータを更新手段が更新する。出力手段が前記保持手段に保持されるデータの一部を、乱数系列として順次出力する。

【0024】また、算出手段が前記パラメータとして出力系列から該系列を推定することが困難なパラメータ系列を順次算出してパラメータを変更する。

【0025】また、送信側で、データを保持する第1の保持部に保持されたデータを第1の変換部に入力し、所定のパラメータに基づいて入力データを変換し、該変換の結果に基づき、前記第1の保持部に保持されるデータを更新し、前記第1の保持部に保持されるデータの一部を、乱数系列として順次出力し、該出力される乱数系列に基づいて通信文を暗号化して暗号文を順次受信側に送信し、受信側で、データを保持する第2の保持部に保持されたデータを第2の変換部に入力し、所定のパラメータに基づいて入力データを変換し、該変換の結果に基づき、前記第2の保持部に保持されるデータを更新し、前記第2の保持部に保持されるデータの一部を、乱数系列として順次出力し、該出力される乱数系列に基づいて暗号文を復号する。

【0026】

【実施例】

（実施例1）図1は、LFSRを用いた乱数発生器のブロック構成を示す図である。シフトレジスタ11及びシフトレジスタ11の各レジスタからの値を線形変換しシフトレジスタ11にフィードバックする線形変換回路12からなる。

【0027】本実施例による乱数発生の手順は以下の通りを行う（ただし手順3. 4. 5は同時に行われる）。

【0028】1. シフトレジスタ11の各レジスタに初期値を設定する。

【0029】2. 線形変換回路12は外部から与えられるパラメータに従って線形変換を決定する。

【0030】3. 各レジスタは与えられた値を右にシフトする。

【0031】4. 最右端のレジスタの値を乱数として出力する。

【0032】5. 各レジスタの値を2. で決定された線形変換に従ってフィードバック変換し、最左端のレジ

タの値とする。

【0033】6. 以下3. 4. 5. を繰り返すが、式（2）による出力乱数列の解析が行えないようにするため、出力される乱数の数とその乱数列の解析に必要な乱数の数（今の場合シフトレジスタの段階の2倍）より大きくなる前に線形変換回路12に入力するパラメータを変更し、線形変換方式を変更する。

【0034】この手順において、手順4. で出力される値の全て又は一部、或いは線形変換回路の出力の全て又は一部が本発明によって発生される乱数となる。線形変換回路にAND回路を利用した場合の乱数発生器を図2に示す。図2において、まずシフトレジスタに初期値を設定する。AND回路に接続されたレジスタの値は、前述のタップ列の値 h_0 、 h_{s-1} 、 \dots 、 h_2 、 h_1 を意味するので、レジスタの値を変更すれば線形変換方式を変更することになる。出力乱数系列の数がシフトレジスタの段数の2倍を越える前にパラメータの変更によってレジスタの値を変更すれば式（2）を解くことができず、乱数列を解析することができない。

【0035】また、手順6. において、出力される乱数の数とその乱数列により決定される線形複雑度の2倍より大きくなった後に線形変換回路に入力するパラメータを変更し、線形変換方式を変更した場合でも、式（2）により解析されるのはその線形変換方式の場合だけであり、従来例のようにそれ以降の全ての乱数系列が解析されるのを防ぐことができるため、パラメータによって線形変換方式を変更した後は安全である。

【0036】（実施例2）LFSRによる乱数発生器では、出力乱数系列の解析に必要な乱数の数はLFSRの段数の2倍であるが、非線形フィードバックシフトレジスタを用いた場合には解析に必要な乱数の数をLFSRの場合以上に大きくすることが可能である。よって、式（2）による出力乱数列の解析に必要なビット数が多くなるので、非線形変換の方式を変えるパラメータの変更周期を大きくすることができるという利点がある。その非線形フィードバックシフトレジスタを用いた実施例を図3に示す。

【0037】図3は本発明による非線形フィードバックシフトレジスタを用いた場合の乱数列発生器を示すブロック図である。シフトレジスタ11及びシフトレジスタ11の各レジスタからの値を非線形変換しシフトレジスタ11にフィードバックする非線形変換回路31からなる。

【0038】本実施例による乱数発生の手順は以下の通りを行う（ただし手順3. 4. 5. は同時に行われる）。

【0039】1. シフトレジスタ11の各レジスタに初期値を設定する。

【0040】2. 非線形変換回路31は外部から与えられるパラメータに従って非線形変換を決定する。

【0041】3. 各レジスタは与えられた値を右にシフトする。

【0042】4. 最右端のレジスタの値を乱数として出力する。

【0043】5. 各レジスタの値を2. で決定された非線形変換に従ってフィードバック変換し、最左端のレジスタの値とする。

【0044】6. 以下3. 4. 5. を繰り返すが、式(2)による出力乱数列の解析が行えないようにするため、出力される乱数の数とその乱数列の解析に必要な乱数の数より大きくなる前に非線形変換回路に入力するパラメータを変更し、非線形変換方式を変更する。

【0045】この手順において、手順4. で出力される値の全て又は一部、或いは非線形変換回路31の出力の全て又は一部が本実施例によって発生される乱数となる。具体的な非線形変換回路31の構成としては、公知の非線形関数の入出力の対応を記憶されたROM等によって実現できる。

【0046】(実施例3) 実施例1. 2. では、本発明をわかりやすく説明するため線形及び非線形フィードバックシフトレジスタを用いた例について述べたが、上記実施例の本質は与えられた初期値をもとに、定められた変換を施してフィードバックすることにより連鎖的に乱数を発生させる乱数発生方式において、該変換における変換方式を外より与えるパラメータによって制御すること、特に変換方式を決定するのに必要なだけの乱数列を出力する前に該変換方式を制御するパラメータを変更し、該変換方式を変更すること、にある。このことから明らかなように、乱数発生方式として線形及び非線形フィードバックシフトレジスタに限らず、種々の方式を用

いることができるのは言うまでもない。

【0047】また、フィードバック変換における変換方式に関しても、外部から与えるパラメータによって制御する場合について述べてきたが、外部から与えるパラメータと内部で生成したパラメータを合成したパラメータによって制御することもできる。

【0048】(実施例4) 図4は、乱数を発生させる手順としてシフトレジスタを用いない場合を示している。

【0049】本実施例では、それぞれ同一のクロックで動作する $R_1 \sim R_n$ の n 個のレジスタ、各レジスタからの出力と最終レジスタ(R_n)からのフィードバック出力とで(非)線形変換を行い次のレジスタに出力する $S_1 \sim S_m$ の m 個の(非)線形変換回路からなる。

【0050】本実施例による乱数発生の手順は以下の通りを行う(ただし手順3. 4. 5. は同時に行われる)。

【0051】1. 各レジスタにそれぞれ初期値を設定する。

【0052】2. $S_1 \sim S_m$ の各(非)線形変換回路は外部から与えられるパラメータに従って(非)線形変換

を決定する。

【0053】3. 最右端のレジスタ(R_n)の値を乱数として出力し、最左端のレジスタ(R_1)の値とする。

【0054】4. 各レジスタは3. において保持していた値を出力すると同時に入力部にある値を保持する。

【0055】5. 各(非)線形変換回路は手前のレジスタから出力された値と R_n からのフィードバック出力とを2. で決定された(非)線形変換によって変換し、後のレジスタに出力する。

【0056】6. 以下3. 4. 5. を繰り返すが、式(2)による出力乱数列の解析が行えないようにするため、出力される乱数の数とその乱数列の解析に必要な乱数の数より大きくなる前に(非)線形変換回路に入力するパラメータを変更し、(非)線形変換方式を変更する。

【0057】この手順において、 R_n の出力の全て又は一部が本実施例によって発生される乱数となる。

【0058】また、上記手順において、各(非)線形変換回路は前述のROM等によって構成することができ、各(非)線形変換回路はそれぞれ異なる(非)線形変換を行っても良い。

【0059】(実施例5) 図5は擬似乱数発生器にDES(Data Encryption Standard)暗号回路を用いる場合の実施例を示している。最近差分解読法と呼ばれる有力な解読法が提案され、DES暗号の安全性に疑問が持たれるようになっており、その対策として鍵を頻繁に変更することが考えられる。DES暗号回路を用いる場合は、DES暗号の鍵を変えることが変換方式を変えることになる。

【0060】(実施例6) 以下の実施例によれば、前述の方式Aを用いた乱数発生器へ与えるパラメータを算出するために方式Bを用いたパラメータ算出回路を有し、このパラメータ算出回路より出力されるパラメータによって乱数発生器における変換方式を制御することによって、方式Aの利点である高速性と方式Bの利点である安全性の2つを実現する乱数列の発生を以下のようにして可能にしたものである。

【0061】方式Aによる乱数発生器に出力される乱数の数が、その乱数列の解析に必要な乱数の数より大きくなる前、或いは等しくなる近辺で前記タプル列の値を変更して乱数発生手段の変換の方式を変更させることにより、式(2)の方法による出力乱数列の解析が行えないようにし、出力乱数系列の安全性を高めることができる。よって、そのタプル列の値をパラメータとして方式Bによって制御する。

【0062】この場合、方式Aを用いた乱数発生器によって出力される乱数の数とその乱数列の解析に必要な乱数の数より大きくなるまでに、方式Bによるパラメータの算出が行われれば良いため、方式Bの計算が高速に行えなくても全体として高速に乱数を生成することは可能

である。

【0063】また、式(2)の方法で解析を行うのに十分な数の乱数を出力した後に前記のタップ列の値を変更したとしても、解析できるのはそのタップ列の値の時だけである。しかもタップ列の値の制御は方式Bによって行われているので次のタップ列の値を予測することは困難であり、従来のようにそれ以降の全ての乱数系列が解析されるのを防ぐことができるため、タップ列の値を変更した後は安全である。

【0064】(実施例7) LFSRによる乱数発生器では、出力乱数系列の解析に必要な乱数の数はLFSRの段数の2倍であるが、非線形フィードバックシフトレジスタを用いた場合には解析に必要な乱数の数をLFSRの場合以上に大きくすることが可能である。よって、式(2)による出力乱数系列の解析に必要なビット数が多くなるので、非線形変換の方式を変えるためのパラメータの算出周期を大きくすることができるという利点がある。算出周期を大きくできることは、高速処理の困難な方式Bをパラメータ算出部に用いる場合に特に大きな利点となる。

【0065】その非線形フィードバックシフトレジスタを用いた実施例を図8に示す。図8は本発明による非線形フィードバックシフトレジスタを用いた場合の乱数発生器を示すブロック図である。方式Aに基づく乱数発生手段としてシフトレジスタ及びシフトレジスタの各レジスタからの値を非線形変換しシフトレジスタにフィードバックする非線形変換回路21を用い、方式Bに基づくパラメータ算出回路61を用いて構成される。非線形変換方式はパラメータ算出回路61からの出力により制御される。

【0066】本実施例による乱数発生手順は以下の通りに行う(ただし手順4. 5. 6. は同時に行われる)。

【0067】1. シフトレジスタの各レジスタ及びパラメータ算出回路に初期値を設定する。

【0068】2. パラメータ算出回路は与えられた初期値から第一のパラメータを算出し、非線形変換回路21に出力する。

【0069】3. 非線形変換回路21は、2. により与えられるパラメータに従って非線形変換を決定する。

【0070】4. 各レジスタは与えられた値を右にシフトする。

【0071】5. 最右端のレジスタの値を乱数として出力する。

【0072】6. 各レジスタの値を3. で決定された非線形変換に従ってフィードバック変換し、最左端のレジスタの値とする。

【0073】7. 以下4. 5. 6. を繰り返すが、式(2)による出力乱数系列の解析が行えないようにするため、出力される乱数の数がその乱数系列の解析に必要な乱数の数より大きくなる前にパラメータ算出回路は次のパ

ラメータを算出し、非線形変換回路21に出力して非線形変換方式を変更する。

【0074】この手順において、手順5. で出力される値の全て又は一部、或いは非線形変換回路の出力の全て又は一部が本発明によって発生される乱数となる。具体的な非線形変換回路21の構成としては、公知の非線形関数の入出力の対応を記憶させたROM等によって実現できる。

【0075】(実施例8) 実施例6, 7では、本発明をわかりやすく説明するため乱数発生手段として線形及び非線形フィードバックシフトレジスタを用いた例について述べたが、本発明の本質は方式Aを用いた乱数発生手段の変換方式を方式Bを用いたパラメータ算出手段から出力されるパラメータによって制御することにある。特に乱数発生手段の変換方式を決定するのに必要なだけの乱数列を出力する前に該変換方式をパラメータ算出手段からの出力により変更することにある。このことから明らかなように、乱数発生手段として線形及び非線形フィードバックシフトレジスタに限らず、種々の方式を用いることができるのは言うまでもない。

【0076】また、方式Bとして用いることのできる暗号学的に安全な擬似乱数発生法には、式(3)の他に文献「暗号と情報セキュリティ」(辻井、笠原著、1990年発行、株式会社昭晃社、86頁)に示されているように、RSA暗号、離散対数、逆数暗号を用いたものが知られており、これらも本発明のパラメータ算出手段のアルゴリズムに用いることができる。

【0077】また、図2のように暗号学的に安全な擬似乱数発生法と内容が秘密にされたROMをフィードバック的に用いる方法を組み合わせることによっても方式Bに基づくパラメータ発生手段は構成できる。

【0078】また、内容が秘密にされたROMをフィードバック的に用いる方法だけでも、それまでにそのROMから発生した値からROM内部の残りの値を知ることとはできないため、方式Bに基づくパラメータ発生手段は構成できる。

【0079】さらに、乱数発生手段の変換方式の制御に関してもパラメータ算出回路により生成されたパラメータによってのみ制御する場合について述べてきたが、乱数発生手段の内部のパラメータとパラメータ算出回路で算出したパラメータとを合成したパラメータによって制御することもできる。

【0080】(実施例9) 図9は、乱数を発生させる手順としてシフトレジスタを用いない場合を示している。

【0081】本実施例では、方式Aに基づく乱数発生手段としてそれぞれ同一のクロックで動作するR₁ ~ R_s のs個のレジスタ及び各レジスタからの出力と最終レジスタ(R_s)からのフィードバック出力とで(非)線形変換を行い次のレジスタに出力するT₁ ~ T_m のm個の(非)線形変換回路を用い、方式Bに基づくパラメータ

算出回路61を用いて構成される。各(非)線形変換方式はパラメータ算出回路61からの出力により制御される。

【0082】本実施例による乱数発生の手順は以下の通りを行う(ただし手順4. 5. 6. は同時に行われる)。

【0083】1. 各レジスタ及びパラメータ算出回路61にそれぞれ初期値を設定する。

【0084】2. パラメータ算出回路61は与えられた初期値から第一のパラメータを算出し、各(非)線形変換回路に出力する。

【0085】3. $T_1 \sim T_n$ の各(非)線形変換回路は2. により与えられるパラメータに従ってそれぞれの(非)線形変換を決定する。

【0086】4. 最右端のレジスタ(R_n)の値を乱数として出力し、最左端のレジスタ(R_1)の値とする。

【0087】5. 各レジスタは4. において保持していた値を出力すると同時に入力部にある値を保持する。

【0088】6. 各(非)線形変換回路は手前のレジスタから出力された値と R_n からのフィードバック出力とを3. で決定された(非)線形変換によって変換し、後のレジスタに出力する。

【0089】7. 以下4. 5. 6. を繰り返すが、式(2)による出力乱数列の解析が行えないようにするため、出力される乱数の数とその乱数列の解析に必要な乱数の数より大きくなる前にパラメータ算出回路は次のパラメータを算出し、各(非)線形変換回路に出力してそれぞれの(非)線形変換方式を変更する。

【0090】この手順において、 R_n の出力の全て又は一部が本発明によって発生される乱数となる。

【0091】また、上記手順において、各(非)線形変換回路は前述のROM等によって構成することができ、各(非)線形変換回路はそれぞれ異なる(非)線形変換を行っても良い。

【0092】(実施例10)図10は本発明において乱数発生手段にDES(Data Encryption Standard)暗号回路51を用いる場合の実施例を示している。最近差分解読法と呼ばれる有力な解読法が提案され、DES暗号の安全性に疑問が持たれるようになっており、その対策として鍵を頻繁に変更することが考えられる。DES暗号装置51を用いる場合は、DES暗号の鍵を変えることが変換方式を変えることになる。

【0093】(実施例11)これまでに述べたように、上記の乱数発生器によって生成された乱数は解析に対して強いので、この乱数を暗号化方式に用いることにより解析に対して強く安全性の高い暗号通信が実現できる。以下、通信文と乱数との間でビット毎に排他的論理和をとる暗号化方式(ストリーム暗号)による暗号通信ネットワークにおいて、乱数発生器を用いた暗号通信の実施

例を示す。

【0094】図11はネットワークの加入者間で固有かつ秘密の暗号鍵を共有している共通鍵暗号通信ネットワークを示し、A、B、C、…、Nはそのネットワークの加入者、 K_{AB} 、 K_{AC} 、…はそれぞれ加入者A-B間で共有している暗号鍵、加入者A-C間で共有している暗号鍵、…を示している。

【0095】図12は本発明による乱数発生回路とパラメータ算出回路からなる乱数発生器121を用いた場合の暗号装置及び復号装置を含む通信装置122の構成を示したブロック図である。

【0096】図13は図11、図12で示された暗号通信システムにおけるA、B間の秘匿通信の様子を示している。

【0097】加入者Aから加入者Bへの暗号通信は以下の手順で行う。

【0098】1. 通信の送信者Aは、送信先Bと共有している秘密の鍵 K_{AB} の全て又は一部を乱数発生回路及びパラメータ算出回路の初期値として設定し、乱数系列 k_i を発生させる。

【0099】2. Aは発生した乱数系列 k_i と通信文 m_i をビット毎に排他的論理和をとり、暗号文

【0100】

【外3】

$$c_i = m_i \oplus k_i$$

を計算し、その暗号文をBに送信する。

【0101】3. 通信の受信者Bは、送信元Aと共有している秘密の鍵 K_{AB} の全て又は一部を乱数発生回路及びパラメータ算出回路の初期値として設定し、送信者が発生したのと同じ乱数系列 k_i を発生させる。

【0102】4. Bは発生した乱数系列 k_i と受信暗号文 c_i をビット毎に排他的論理和をとり、通信文

【0103】

【外4】

$$m_i = c_i \oplus k_i$$

を復元する。

【0104】この手順に従えば、正規の送信先Bだけがその秘密の鍵 K_{AB} を知っているので受け取った暗号文を本来の通信文に復号でき、それ以外の加入者(C~N)はその暗号文をする際に用いられた秘密の鍵を知らないものでその内容を知ることができない。このことにより秘匿通信が実現される。また、図11のようにあらかじめ暗号鍵が配布されているのではなく、暗号通信を行うに先立って送・受信者間で暗号鍵を共有する必要がある形態のネットワークにおいても、公知の手法で鍵共有を行えば同じ手順で暗号通信を実現することができる。

【0105】(実施例12)実施例11に示した暗号通信ネットワークでは通信文の送信者と受信者の間で固有

かつ秘密の鍵を共有しているので、暗号文を受け取り、意味をなす通信文に復号できるということは、通信文がその鍵のもう一人の所有者から送信されたことを受信者に保証している。そのため、実施例11に示した秘匿通信システムでは、通信の発信者及び着信者の認証も行うことができる。

【0106】（実施例13）実施例11、12のようにあらかじめ暗号鍵が配布されているのではなく、暗号通信を行うに先立って送・受信者間で暗号鍵を共有する必要がある形態のネットワークにおいて、盗聴の可能性のある通信路を介した場合でも安全に暗号鍵を共有できる方式としてDiffie-Hellmanの方式（W. Diffie and M. E. Hellman “New Directions in cryptography”, IEEE, IT, vol. I, T-22, No. 6, 1976）がよく知られている。その際に用いる乱数として本発明により発生した乱数を用いることができる。

【0107】その場合に用いる乱数は、送信者と着信者で同じものを持つ必要はないため、乱数発生手段及びパラメータ発生手段に設定する初期値は任意の値を用いれば良い。

【0108】

【発明の効果】以上説明したように、本発明によれば、一定数の出力系列から解析可能な方式（方式A）により出力される乱数の数が、その解析に必要な数より大きくなる前、或いは等しくなる近辺で、方式Aのパラメータを変更するので、方式Aの解析に必要な数の出力を集めることが困難になり、発生する乱数の安全性が高められるという効果がある。

【0109】また、方式Aのパラメータを、出力系列から解析困難な方式（方式B）により出力される乱数に基づいて変更することにより、方式Aの安全性が一層高められるという効果がある。

【0110】この場合、方式Aから出力される出力の数が方式Aの解析に必要な数より大きくなるまでに、方式Bによる乱数の出力が行われれば良いため、方式Bの乱数発生は高速に行えなくてもよい。しかし、最終出力は方式Aからの出力であるので、高速に乱数を発生することが可能である。

【0111】また、この乱数系列を暗号通信に用いれば、高速かつ安全性の高い暗号通信が実現されるという

効果がある。

【図面の簡単な説明】

【図1】LFSRを用いた乱数発生器のブロック構成を示す図である。

【図2】LFSRを用いた乱数発生器の詳細なブロック構成を示す図である。

【図3】非線形フィードバックレジスタを用いた乱数発生器のブロック構成を示す図である。

【図4】複数のレジスタを用いた乱数発生器のブロック構成を示す図である。

【図5】DES暗号装置を用いた乱数発生器のブロック構成を示す図である。

【図6】LFSRを用いた乱数発生器のブロック構成を示す図である。

【図7】LFSRを用いた乱数発生器のブロック構成を示す図である。

【図8】非線形フィードバックレジスタを用いた乱数発生器のブロック構成を示す図である。

【図9】複数のレジスタを用いた乱数発生器のブロック構成を示す図である。

【図10】DES暗号装置を用いた乱数発生器のブロック構成を示す図である。

【図11】共通鍵暗号通信ネットワークを説明する図である。

【図12】暗号装置及び復号装置を含む通信装置の構成を示すブロック図である。

【図13】秘匿通信を行う通信システムを説明する図である。

【図14】LFSRを用いた従来の乱数発生器のブロック構成を示す図である。

【符号の説明】

11 シフトレジスタ

12 線形変換回路

21 レジスタ

31 非線形変換回路

51 DES暗号回路

61 パラメータ算出回路

71 ROM

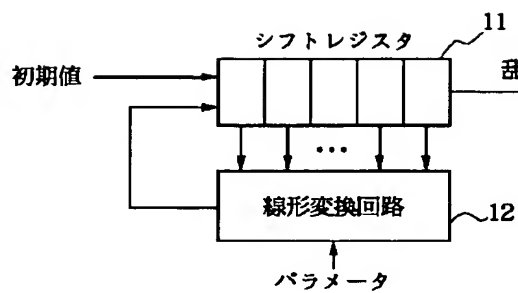
72 バッファ

73 自乗剰余算回路

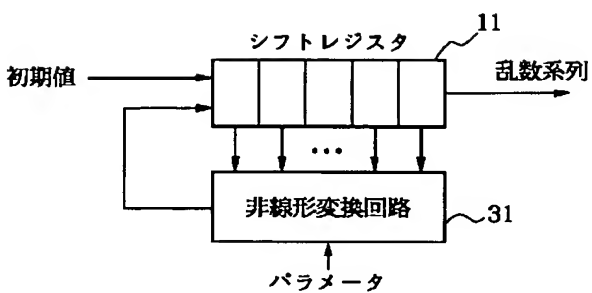
121 乱数発生器

122 通信装置

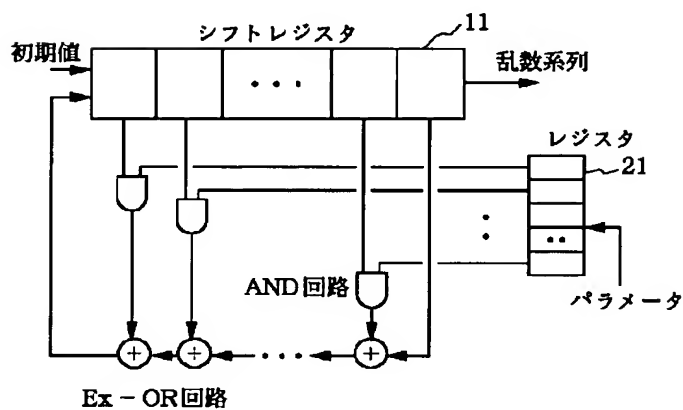
【図 1】



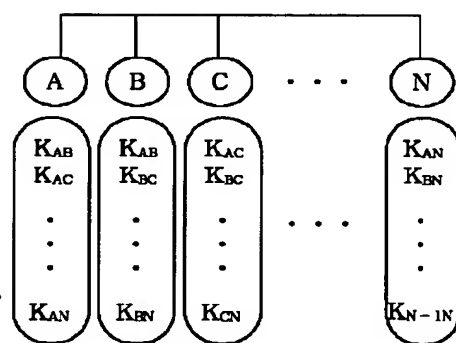
【図 3】



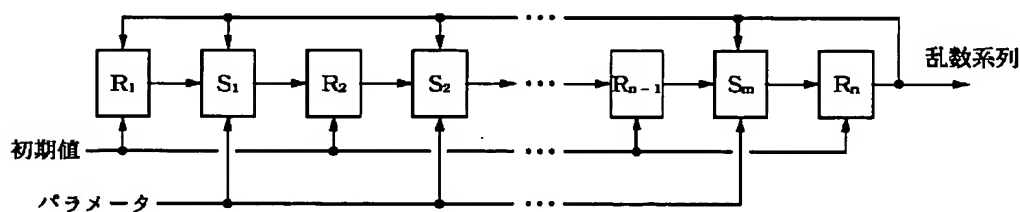
【図 2】



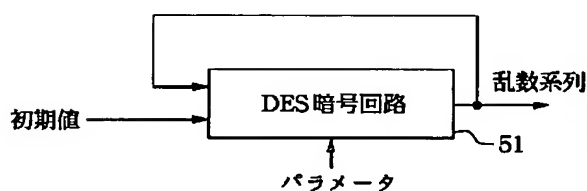
【図 11】



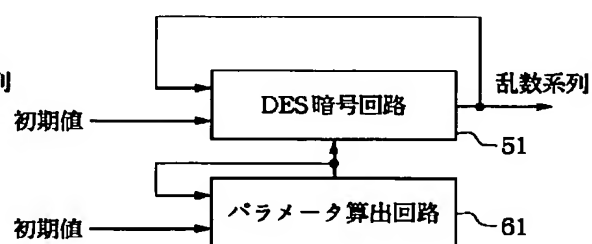
【図 4】



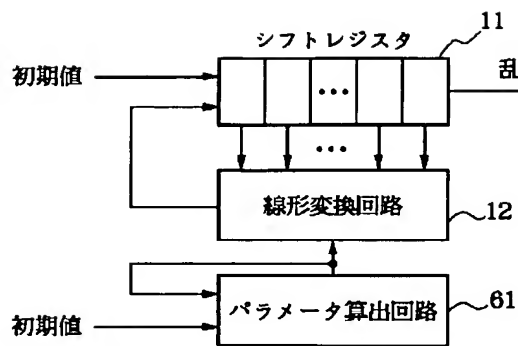
【図 5】



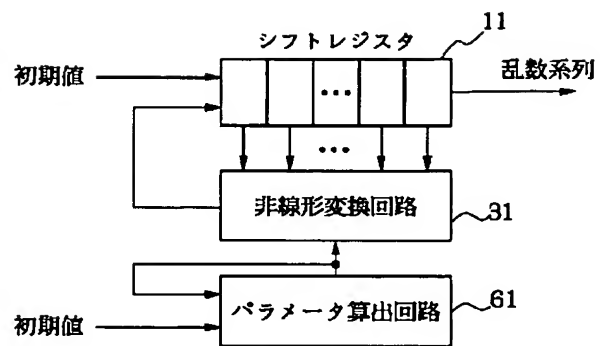
【図 10】



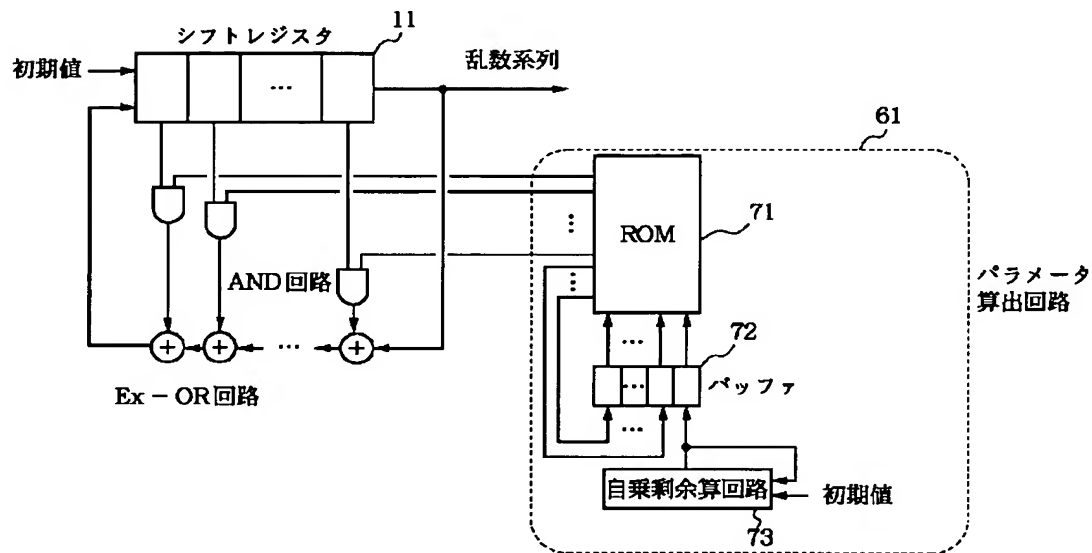
【図6】



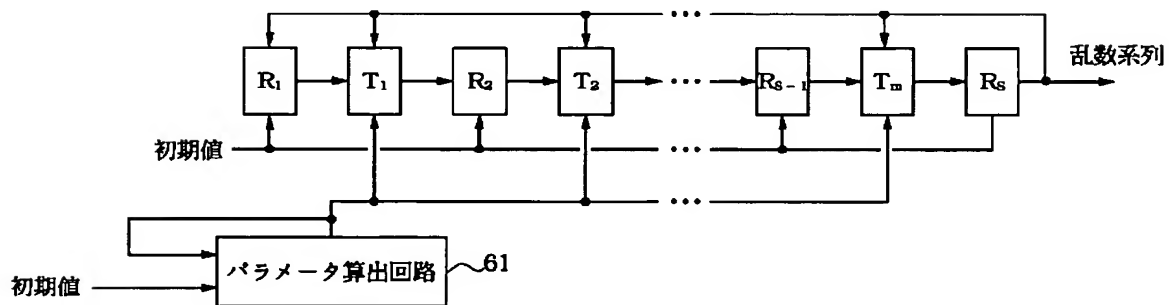
【図8】



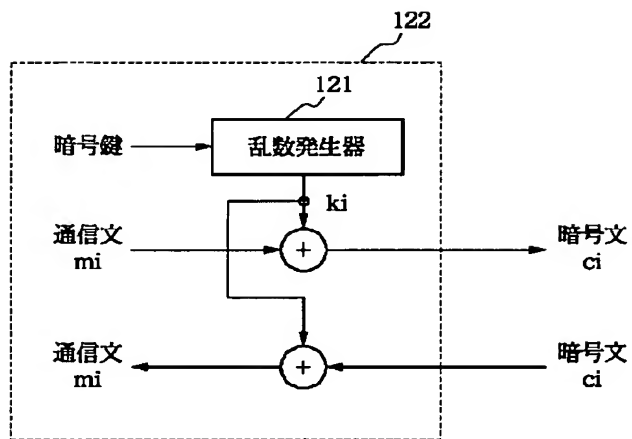
【図7】



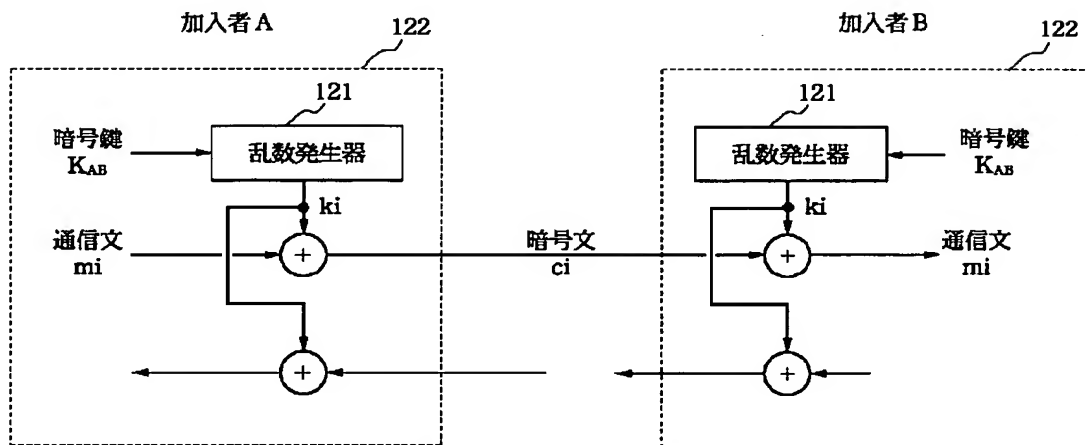
【図9】



【図12】



【図13】



【図14】

